

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開2002-245414  
(P2002-245414A)

(43)公開日 平成14年8月30日(2002.8.30)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
G 0 6 K 17/00		G 0 6 K 17/00	B 5 B 0 5 8
G 0 6 F 1/00		G 0 6 F 15/00	3 3 0 C 5 B 0 7 6
15/00	3 3 0	9/06	6 6 0 D 5 B 0 8 5

審査請求 未請求 請求項の数23 O L (全 16 頁)

(21)出願番号 特願2001-40415(P2001-40415)

(22)出願日 平成13年2月16日(2001.2.16)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 末吉 正弘

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 久保野 文夫

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74)代理人 100094053

弁理士 佐藤 隆久

Fターム(参考) 5B058 CA01 KA11

5B076 FB05 FB10

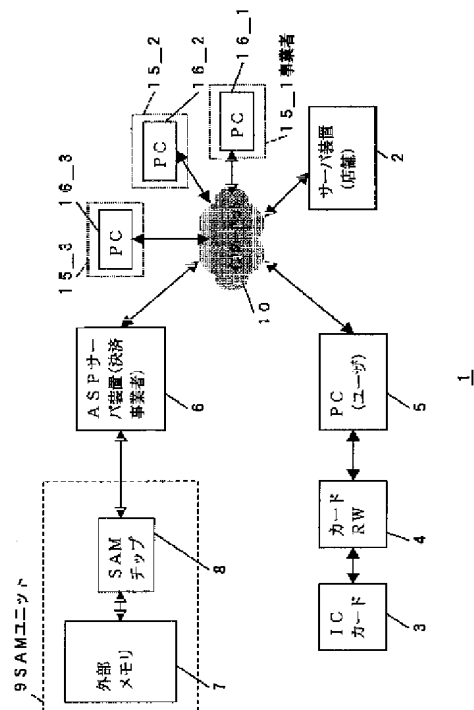
5B085 AE12 BG07 CC06

(54)【発明の名称】 データ処理方法および半導体回路

(57)【要約】

【課題】 秘匿性の高い情報をユーザに知らせることなく、サーバ装置で実行するユーザのアプリケーションプログラムを当該ユーザが作成およびカスタマイズできるデータ処理方法を提供する。

【解決手段】 アプリケーションプログラムAPがICカード3を操作するために用いる操作コードと操作の名前である操作名との対応を示すテーブルをSAMチップ8が参照可能であり、APの動作を操作名を用いて記述したスクリプトプログラムをSAMチップ8が入力する。SAMチップ8は、スクリプトプログラムに記述された操作名に対応する操作コードをテーブルを参照して得て、当該得た操作コードを用いてAPの処理を規定する。



## 【特許請求の範囲】

【請求項1】集積回路を用いた手続きに関する処理を行うアプリケーションプログラムが動作する半導体回路が行うデータ処理方法であって、前記アプリケーションプログラムが前記集積回路を操作するために用いる操作コードと前記操作の名前である操作名との対応を示す対応指示データを前記半導体回路が参照可能であり、前記アプリケーションプログラムの動作を前記操作名を用いて記述した動作記述プログラムを前記半導体回路が入力し、前記半導体回路が、前記動作記述プログラムに記述された前記操作名に対応する前記操作コードを前記対応指示データを参照して得て、当該得た操作コードを用いて前記アプリケーションプログラムの処理を規定するデータ処理方法。

【請求項2】前記対応指示データは、前記操作名と、当該操作名に対応する操作を前記集積回路に行うときに用いられる鍵情報との対応をさらに示し、前記半導体回路は、前記動作記述プログラムに記述された前記操作名に対応する前記鍵情報を前記対応指示データを参照して得て、当該得た鍵情報を用いて前記アプリケーションプログラムの処理を規定するデータ処理方法。

【請求項3】前記半導体回路は、処理要求に応じて、前記アプリケーションプログラムの処理を構成する複数のジョブの実行順番を示すジョブ実行順番データと、前記複数のジョブの実行の進行状態を示すステータスデータとを含むジョブ管理用データを生成し、前記ジョブ管理用データの前記ステータスデータおよび前記処理順番データに基づいて、次に実行を行うジョブを選択し、前記選択したジョブを実行し、当該ジョブの実行に応じて、前記選択したジョブ管理用データの前記ステータスデータを更新する請求項1に記載のデータ処理方法。

【請求項4】前記半導体回路は、前記対応指示データおよび前記動作記述プログラムを用いて、前記ジョブ管理用データのテンプレートデータを生成し、前記処理要求に応じて、前記テンプレートデータを用いて前記ジョブ管理用データを生成する請求項3に記載のデータ処理方法。

【請求項5】前記半導体回路は、複数の処理要求のそれぞれについて、前記ジョブ管理用データを生成し、複数の前記データモジュールから一つのジョブ管理用データを選択し、前記選択したジョブ管理用データの前記ステータスデー

タおよび前記処理順番データに基づいて、次に実行を行うジョブを選択し、前記選択したジョブを実行し、当該ジョブの実行に応じて、前記選択したジョブ管理用データの前記ステータスデータを更新し、当該更新後に、前記複数のデータモジュールから一つのジョブ管理用データを選択する請求項3に記載のデータ処理方法。

【請求項6】前記半導体回路は、前記処理要求に応じた処理を構成する全てのジョブの実行が終了した前記ジョブ管理用データを消去する請求項5に記載のデータ処理方法。

【請求項7】前記動作記述プログラムは、前記半導体回路が処理可能な前記ジョブ管理用データの最大数を指定した記述を含み、前記半導体回路は、前記ジョブ管理用データの数が前記指定された最大数以下の場合に、前記処理要求に応じて前記ジョブ管理用データを生成する請求項5に記載のデータ処理方法。

【請求項8】前記半導体回路は、前記集積回路に対しての複数の前記操作に対応する複数のジョブの実行順番を示す前記実行順番データを含む前記ジョブ管理用データを生成する請求項5に記載のデータ処理方法。

【請求項9】前記動作記述プログラムは、前記集積回路からの読み出したデータを格納するデータブロック、前記集積回路に書き込むデータを格納するデータブロック、および、前記集積回路を用いた手続き処理の履歴情報を格納するデータブロックの少なくとも一つのデータブロックを定義する記述を含み、前記半導体回路は、前記動作記述プログラムに基づいて、前記データブロックを生成する請求項5に記載のデータ処理方法。

【請求項10】前記操作名は、マクロコマンドである請求項1に記載のデータ処理方法。

【請求項11】前記集積回路は、カードに搭載されている請求項1に記載のデータ処理方法。

【請求項12】集積回路を用いた手続きに関する処理を行うアプリケーションプログラムが動作する半導体回路であって、

前記アプリケーションプログラムが前記集積回路を操作するために用いる操作コードと前記操作の名前である操作名との対応を示す対応指示データを参照可能であり、前記アプリケーションプログラムの動作を前記操作名を用いて記述した動作記述プログラムを入力し、当該入力した前記動作記述プログラムに記述された前記操作名に対応する前記操作コードを前記対応指示データを参照して得て、当該得た操作コードを用いて前記アプリケーションプログラムの処理を規定する半導体回路。

【請求項13】前記対応指示データは、前記操作名と、

当該操作名に対応する操作を前記集積回路に行うときに用いられる鍵情報との対応をさらに示し、前記動作記述プログラムに記述された前記操作名に対応する前記鍵情報を前記対応指示データを参照して得て、当該得た鍵情報を用いて前記アプリケーションプログラムの処理を規定する半導体回路。

【請求項14】処理要求に応じて、前記アプリケーションプログラムの処理を構成する複数のジョブの実行順番を示すジョブ実行順番データと、前記複数のジョブの実行の進行状態を示すステータスデータとを含むジョブ管理用データを生成し、前記ジョブ管理用データの前記ステータスデータおよび前記処理順番データに基づいて、次に実行を行うジョブを選択し、前記選択したジョブを実行し、当該ジョブの実行に応じて、前記選択したジョブ管理用データの前記ステータスデータを更新する請求項12に記載の半導体回路。

【請求項15】前記対応指示データおよび前記動作記述プログラムを用いて、前記ジョブ管理用データのテンプレートデータを生成し、前記処理要求に応じて、前記テンプレートデータを用いて前記ジョブ管理用データを生成する請求項14に記載の半導体回路。

【請求項16】複数の処理要求のそれぞれについて、前記ジョブ管理用データを生成し、複数の前記データモジュールから一つのジョブ管理用データを選択し、前記選択したジョブ管理用データの前記ステータスデータおよび前記処理順番データに基づいて、次に実行を行うジョブを選択し、前記選択したジョブを実行し、当該ジョブの実行に応じて、前記選択したジョブ管理用データの前記ステータスデータを更新し、当該更新後に、前記複数のデータモジュールから一つのジョブ管理用データを選択する請求項14に記載の半導体回路。

【請求項17】前記処理要求に応じた処理を構成する全てのジョブの実行が終了した前記ジョブ管理用データを消去する請求項16に記載の半導体回路。

【請求項18】前記動作記述プログラムが、前記半導体回路が処理可能な前記ジョブ管理用データの最大数を指定した記述を含む場合に、前記ジョブ管理用データの数の前記指定された最大数以下であることを条件に、前記処理要求に応じて前記ジョブ管理用データを生成する請求項16に記載の半導体回路。

【請求項19】前記集積回路に対しての複数の前記操作に対応する複数のジョブの実行順番を示す前記実行順番データを含む前記ジョブ管理用データを生成する請求項

16に記載の半導体回路。

【請求項20】前記動作記述プログラムが、前記集積回路からの読み出したデータを格納するデータブロック、前記集積回路に書き込むデータを格納するデータブロック、および、前記集積回路を用いた手続き処理の履歴情報を格納するデータブロックの少なくとも一つのデータブロックを定義する記述を含む場合に、前記動作記述プログラムに基づいて、前記データブロックを生成する請求項16に記載の半導体回路。

【請求項21】前記操作名は、マクロコマンドである請求項16に記載の半導体回路。

【請求項22】前記集積回路は、カードに搭載されている請求項16に記載の半導体回路。

【請求項23】耐タンパ性の半導体回路である請求項16に記載の半導体回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、所定の情報の秘匿性を保ちながら、アプリケーションプログラムのカスタマイズを行うことを可能にするデータ処理方法および半導体回路に関する。

【0002】

【従来の技術】現在、ICカードを用いてインターネットなどのネットワークを介した取り引きを行う通信システムが開発されている。このような通信システムでは、ICカードを用いたサービスを提供するサービス提供者からの依頼を受けて当該サービス提供者が規定した手続き処理を実行するアプリケーションプログラムをサーバ装置が実行する。サーバ装置は、例えばICカードのリーダー・ライターやPC(Personal Computer)から処理要求に応じて、上記アプリケーションプログラムに基づいて、ユーザ認証やデータの暗号化及び復号などの処理を行う。このようなアプリケーションプログラムは、ICカードにアクセスを行うための鍵情報やICカードを操作するための操作コマンドを用いてコードを記述する必要がある。ここで、これらの鍵情報や操作コマンドは、ICカードを用いた取り引きの安全性を期す上で上記サーバ装置の管理者のみが知ることができる。従って、従来では、サーバ装置の管理者が、上記サービス提供者から依頼を受けて、上記アプリケーションプログラムを作成およびカスタマイズしている。

【0003】

【発明が解決しようとする課題】しかしながら、上述したようにサーバ装置の管理者がアプリケーションプログラムの作成およびカスタマイズを行うのでは、当該管理者の負担を大きいという問題がある。

【0004】本発明は上述した従来技術の問題点を鑑みてなされ、秘匿性の高い情報をユーザに知らせることなく、サーバ装置で実行するユーザのアプリケーションプログラムを当該ユーザが作成およびカスタマイズできる

データ処理方法および半導体回路を提供することを目的とする。

【0005】

【課題を解決するための手段】上述した目的を達成するために、本発明のデータ処理方法は、集積回路を用いた手続きに関する処理を行うアプリケーションプログラムが動作する半導体回路が行うデータ処理方法であって、前記アプリケーションプログラムが前記集積回路を操作するために用いる操作コードと前記操作の名前である操作名との対応を示す対応指示データを前記半導体回路が参照可能であり、前記アプリケーションプログラムの動作を前記操作名を用いて記述した動作記述プログラムを前記半導体回路が入力し、前記半導体回路が、前記動作記述プログラムに記述された前記操作名に対応する前記操作コードを前記対応指示データを参照して得て、当該得た操作コードを用いて前記アプリケーションプログラムの処理を規定する。

【0006】また、本発明のデータ処理方法は、好ましくは、前記対応指示データは、前記操作名と、当該操作名に対応する操作を前記集積回路に行うときに用いられる鍵情報との対応をさらに示し、前記半導体回路は、前記動作記述プログラムに記述された前記操作名に対応する前記鍵情報を前記対応指示データを参照して得て、当該得た鍵情報を用いて前記アプリケーションプログラムの処理を規定する。

【0007】また、本発明のデータ処理方法は、好ましくは、前記半導体回路は、処理要求に応じて、前記アプリケーションプログラムの処理を構成する複数のジョブの実行順番を示すジョブ実行順番データと、前記複数のジョブの実行の進行状態を示すステータスデータとを含むジョブ管理用データを生成し、前記ジョブ管理用データの前記ステータスデータおよび前記処理順番データに基づいて、次に実行を行うジョブを選択し、前記選択したジョブを実行し、当該ジョブの実行に応じて、前記選択したジョブ管理用データの前記ステータスデータを更新する。

【0008】また、本発明のデータ処理方法は、好ましくは、前記半導体回路は、前記対応指示データおよび前記動作記述プログラムを用いて、前記ジョブ管理用データのテンプレートデータを生成し、前記処理要求に応じて、前記テンプレートデータを用いて前記ジョブ管理用データを生成する。

【0009】また、本発明のデータ処理方法は、好ましくは、前記半導体回路は、複数の処理要求のそれぞれについて、前記ジョブ管理用データを生成し、複数の前記データモジュールから一つのジョブ管理用データを選択し、前記選択したジョブ管理用データの前記ステータスデータおよび前記処理順番データに基づいて、次に実行を行うジョブを選択し、前記選択したジョブを実行し、当該ジョブの実行に応じて、前記選択したジョブ管理用

データの前記ステータスデータを更新し、当該更新後に、前記複数のデータモジュールから一つのジョブ管理用データを選択する。

【0010】また、本発明のデータ処理方法は、好ましくは、前記半導体回路は、前記処理要求に応じた処理を構成する全てのジョブの実行が終了した前記ジョブ管理用データを消去する。

【0011】また、本発明のデータ処理方法は、好ましくは、前記動作記述プログラムは、前記半導体回路が処理可能な前記ジョブ管理用データの最大数を指定した記述を含み、前記半導体回路は、前記ジョブ管理用データの数が前記指定された最大数以下の場合に、前記処理要求に応じて前記ジョブ管理用データを生成する。

【0012】また、本発明のデータ処理方法は、好ましくは、前記半導体回路は、前記集積回路に対しての複数の前記操作に対応する複数のジョブの実行順番を示す前記実行順番データを含む前記ジョブ管理用データを生成する。

【0013】また、本発明のデータ処理方法は、好ましくは、前記動作記述プログラムは、前記集積回路からの読み出したデータを格納するデータブロック、前記集積回路に書き込むデータを格納するデータブロック、および、前記集積回路を用いた手続き処理の履歴情報を格納するデータブロックの少なくとも一つのデータブロックを定義する記述を含み、前記半導体回路は、前記動作記述プログラムに基づいて、前記データブロックを生成する。

【0014】また、本発明のデータ処理方法は、好ましくは、前記操作名は、マクロコマンドである。

【0015】また、本発明のデータ処理方法は、好ましくは、前記集積回路は、カードに搭載されている。

【0016】また、本発明の半導体回路は、集積回路を用いた手続きに関する処理を行うアプリケーションプログラムが動作する半導体回路であって、前記アプリケーションプログラムが前記集積回路を操作するために用いる操作コードと前記操作の名前である操作名との対応を示す対応指示データを参照可能であり、前記アプリケーションプログラムの動作を前記操作名を用いて記述した動作記述プログラムを入力し、当該入力した前記動作記述プログラムに記述された前記操作名に対応する前記操作コードを前記対応指示データを参照して得て、当該得た操作コードを用いて前記アプリケーションプログラムの処理を規定する。

【0017】

【発明の実施の形態】以下、本発明の実施の形態を添付図面を参照して説明する。図1は、本実施形態の通信システム1の全体構成図である。図1に示すように、通信システム1は、サーバ装置2、ICカード3、カードリーダー・ライタ4、パーソナルコンピュータ5、ASP (Application Service Provider)サーバ装置6、SAM (S

ecure Application Module) ユニット9を用いて、インターネット10を介して通信を行ってICカード3(本発明の集積回路)を用いた決済処理などの手続き処理を行う。SAMユニット9は、外部メモリ7およびSAMチップ(本発明の半導体回路)8を有する。

【0018】SAMチップ8は、図2に示すようなソフトウェア構成を有している。図2に示すように、SAMチップ8は、下層から上層に向けて、HW(Hardware)層、OS層、下位ハンドラ層、上位ハンドラ層およびAP層を順に有している。下位ハンドラ層には、ドライバ層が含まれる。ここで、AP層には、図1に示すクレジットカード会社などの事業者15\_1、15\_2、15\_3によるICカード3を用いた手続きを規定したアプリケーションプログラムAP\_1、AP\_2、AP\_3がある。AP層では、アプリケーションプログラムAP\_1、AP\_2、AP\_3相互間、並びに上位ハンドラ層との間にファイアウォールFWが設けられている。

【0019】アプリケーションプログラムAP\_1は、外部メモリ7に記憶された後述するサービス定義テーブルデータ(対応指示データ)20\_1およびスクリプトプログラム(動作記述プログラム)21\_1によって規定される。また、アプリケーションプログラムAP\_2は、外部メモリ7に記憶された後述するサービス定義テーブルデータ20\_2およびスクリプトプログラム21\_2によって規定される。また、アプリケーションプログラムAP\_3は、外部メモリ7に記憶された後述するサービス定義テーブルデータ20\_3およびスクリプトプログラム21\_3によって規定される。

【0020】SAMチップ8は、SCSIまたはEthernetなどを介してASPサーバ装置6に接続される。ASPサーバ装置6は、インターネット10を介して、エンドユーザのパーソナルコンピュータ5、事業者15\_1、15\_2、15\_3のパーソナルコンピュータ16\_1、16\_2、16\_3を含む複数の端末装置に接続される。パーソナルコンピュータ5は、例えば、シリアルまたはUSBを介してDumb型のカードリーダー・ライタ4に接続されている。カードリーダー・ライタ4が、ICカード3との間で物理レベルに相当する例えば無線通信を実現する。ICカード3への操作コマンドおよびICカード3からのレスポンスパケットは、SAMユニット9側で生成および解釈される。よって、その中間に介在するカードリーダー・ライタ4、パーソナルコンピュータ5およびASPサーバ装置6は、コマンドやレスポンス内容をデータペイロード部分に格納して中継する役割を果たすのみで、ICカード3内のデータの暗号化や復号および認証などの実操作には関与しない。

【0021】パーソナルコンピュータ16\_1、16\_2、16\_3は、後述するスクリプトプログラムをSAMチップ8にダウンロードすることで、それぞれアプリケーションプログラムAP\_1、AP\_2、AP\_3を

カスタマイズできる。

【0022】以下、図1に示す構成要素について説明する。

〔ICカード3〕図3は、ICカード3の機能ブロック図である。図3に示すように、ICカード3は、記憶部50および処理部51を備えたIC(Integrated Circuit)3aを有する。記憶部50は、図4に示すように、クレジットカード会社などの事業者15\_1が使用する記憶領域55\_1、事業者15\_2が使用する記憶領域55\_2、並びに事業者15\_3が使用する記憶領域55\_3を有する。また、記憶部50は、記憶領域55\_1へのアクセス権限を判断するために用いられる鍵情報、記憶領域55\_2へのアクセス権限を判断するために用いられる鍵情報、並びに記憶領域55\_3へのアクセス権限を判断するために用いられる鍵情報を記憶している。当該鍵情報は、相互認証や、データの暗号化および復号などに用いられる。また、記憶部50は、ICカード3あるいはICカード3のユーザの識別情報を記憶している。

【0023】以下、SAMユニット9について詳細に説明する。

〔外部メモリ7〕図5は、図1に示す外部メモリ7に記憶されるデータおよびプログラムを説明するための図である。図5に示すように、外部メモリ7には、事業者15\_1のサービス定義テーブルデータ20\_1と、ICカード操作用マクロコマンドスクリプトプログラム21\_1とが記憶されている。また、外部メモリ7には、事業者15\_2のサービス定義テーブルデータ20\_2と、ICカード操作用マクロコマンドスクリプトプログラム21\_2とが記憶されている。また、外部メモリ7には、事業者15\_3のサービス定義テーブルデータ20\_3と、ICカード操作用マクロコマンドスクリプトプログラム21\_3とが記憶されている。サービス定義テーブルデータ20\_1、20\_2、20\_3は、同じフォーマットを有している。また、ICカード操作用マクロコマンドスクリプトプログラム21\_1、21\_2、21\_3は、共通のマクロコマンドを用いて記述されている。また、サービス定義テーブルデータ20\_1、20\_2、20\_3およびICカード操作用マクロコマンドスクリプトプログラム21\_1、21\_2、21\_3は、スクランブルされて外部メモリ7に記憶されている。当該スクランブルされたデータおよびプログラムは、SAMチップ8内でデスクランブルされる。

【0024】本実施形態では、スクリプトプログラム21\_1、21\_2、21\_3は、それぞれ図1に示すパーソナルコンピュータ16\_1、16\_2、16\_3を用いて、事業者15\_1、15\_2、15\_3によって作成され、SAMチップ8を介して外部メモリ7にダウンロードされる。また、サービス定義テーブルデータ20\_1、20\_2、20\_3は、それぞれ事業者15\_

1, 15\_2, 15\_3からの指示を受けてSAMユニット9の管理者によって作成される。

【0025】図6は、サービス定義テーブルデータ20\_1を説明するための図である。図6に示すように、サービス定義テーブルデータ20\_1は、サービスタイプエレメント（操作名）、アドレス、サービス番号（操作コード）、鍵バージョン情報、並びに鍵情報のエントリを有している。サービスタイプエレメントは、事業者15\_1のアプリケーションプログラムによって提供されるサービスに付けられた名前を示す。サービスタイプエレメントは、事業者15\_1のアプリケーションプログラムが使用できるサービスのサービス番号の替わりに参照される識別子である。本実施形態では、図6に示すように、事業者15\_1に対応するサービス定義テーブルデータ20\_1のサービスタイプエレメントとしては、“Rc”、“Rd”、“Wd”および“Wc”が用いられている。本実施形態では、ICカード操作マクロコマンドスクリプトプログラム21\_1において、複数のサービスタイプエレメントを組み合わせたサービス内容を規定し、これを後述するICカードエンティティデータ（ジョブ管理用データ）に反映させることで、複数のサービスタイプエレメントに対応するサービスを組み合わせたサービスを提供できる。例えば、ICカード3からデータ読出しを行うサービスと、サーバ装置2にデータ書込みを行うサービスとを組み合わせたサービスを、ICカードエンティティデータ内に定義できる。

【0026】サービス定義テーブルデータ20\_1内のサービス番号は、事業者15\_1によって提供されるサービスを行う際に、ICカード3に発行するICカード3が解釈可能な操作コマンドである。

【0027】サービス定義テーブルデータ20\_1内のアドレスは、対応するサービスタイプエレメントに係わる手続きに関するデータが記憶されているアドレスを示している。サービス定義テーブルデータ20\_1内の鍵バージョン情報は、当該サービスを提供するにあたって用いられる鍵情報のバージョンを示している。サービス定義テーブルデータ20\_1内の鍵情報は、当該サービスを提供するにあたって用いられる鍵情報である。例えば、サービス定義テーブルデータ20\_1では、図3に示すICカード3のIC3aの記憶領域55\_1にアクセスが行われる際に用いられる鍵情報が設定されている。また、サービス定義テーブルデータ20\_2では、IC3aの記憶領域55\_2にアクセスが行われる際に用いられる鍵情報が設定されている。また、サービス定義テーブルデータ20\_3では、IC3aの記憶領域55\_3にアクセスが行われる際に用いられる鍵情報が設定されている。

【0028】以下、ICカード操作マクロコマンドスクリプトプログラム21\_1について説明する。スクリプトプログラム21\_1は、SAMチップ8上で動作す

る事業者15\_1のアプリケーションプログラム、並びに当該アプリケーションプログラムの実行時にICカード3が行う処理の手続きを規定するためのプログラムである。本実施形態では、後述するように、図7に示すように、SAMチップ8内で、サービス定義テーブルデータ20\_1およびスクリプトプログラム21\_1を用いて、事業者15\_1に関する手続きに用いられるICカードエンティティテンプレートデータ30\_1、入力用データブロック31\_x1、出力用データブロック32\_x2、ログ用データブロック33\_x3および演算定義用データブロック34\_x4が生成される。

【0029】図8は、ICカード操作マクロコマンドスクリプトプログラム21\_1、21\_2、21\_3の記述に用いられるコマンドを説明するための図である。当該コマンドは、SAMチップ8自身に対してのコマンドは、第1文字が「S」となり、ICカード3の操作に係わるコマンドは第1文字が「C」となっている。また、第2文字は、用途により使い分けられ、例えば、ICカード3の発行元設定宣言は「I」、サービスタイプエレメント宣言は「S」、ICカード3からの単純読み込み宣言は「R」、ICカード3への単純書き込み宣言は「W」、サービスタイプエレメント間演算定義は「F」になっている。

【0030】スクリプトプログラム21\_1、21\_2、21\_3の記述に用いられるコマンドには、SCコマンド、SOコマンド、SIコマンド、SLコマンド、SFコマンド、CIコマンド、CSコマンド、CRコマンド、CWコマンドがある。SCコマンドは、SAMチップ8が同時に処理することができる最大数のICカードエンティティデータの数を宣言するコマンドである。例えば、SAMチップ8が1000個のICカードエンティティデータを同時に処理可能な場合には、「SC:1000」と記述される。

【0031】SOコマンドは、後述するICカードエンティティデータに基づいてICカード3を用いた処理を行う際に、SAMチップ8内で用意されたデータブロックのうち、ICカード3から読み取ったデータが格納される出力用データブロック32\_x2となるデータブロックを宣言するコマンドである。例えば、データブロック1~10が用意されている場合に、ICカード3から読み取ったデータをデータブロック1に格納する場合には、「SO:1」と記述される。

【0032】SIコマンドは、後述するICカードエンティティデータに基づいてICカード3を用いた処理を行う際に、SAMチップ8内で用意されたデータブロックのうち、ICカード3に書き込むデータが格納される入力用データブロック31\_x1となるデータブロックを宣言するコマンドである。例えば、データブロック1~10が用意されている場合に、ICカード3に書き込むデータをデータブロック2、3に格納する場合には、

「SI: 2, 3」と記述される。

【0033】SLコマンドは、後述するICカードエンティティデータに基づいてICカード3を用いた処理を行う際に、SAMチップ8内で用意されたデータブロックのうち、操作に係わるログデータを格納するログ用データブロック33\_\_x3となるデータブロックを宣言するコマンドである。例えば、データブロック1～10が用意されている場合に、ログデータをデータブロック4に格納する場合には、「SL: 4」と記述される。

【0034】SFコマンドは、ICカード3に係わる相互のサービスタイプエレメント間の関係を定義を記述する演算定義用データブロック34\_\_x4となるデータブロックを用意するためのコマンドである。演算定義用データブロック34\_\_x4の内容は、ICカードエンティティデータの処理前情報となる。

【0035】CIコマンドは、ICカード3の発行元（事業者）を宣言するためのコマンドである。CIコマンドで定義された事業者を特定する情報は、ICカードエンティティデータのICカード種別情報となる。

【0036】CSコマンドは、サービスタイプエレメントを引用して、ICカード3への複数のサービスの同時操作を行うことを宣言するコマンドである。CSコマンドでは、さらに、サービスタイプエレメント間の演算を規定する関数を宣言できる。例えば、「CS: "Rc" + "Wc" + "Wd"」などの宣言を行える。CSコマンドの内容に基づいて、ICカードエンティティデータのサービスタイプエレメント指定情報、並びに処理順番情報が決定される。

【0037】CRコマンドは、サービスタイプエレメント間の関係の定義が行われていない場合（SFコマンドが記述されていない場合）に、ICカード3から読み出したデータを指定したデータブロックに格納することを宣言する。例えば、ICカード3から読み出したデータをデータブロック1に格納する場合には「CR: SO: 1= "Rc"」と記述する。

【0038】CWコマンドは、サービスタイプエレメント間の関係の定義が行われていない場合に、指定したデータブロックに格納したデータをICカード3に書き込むことを宣言する。例えば、データブロック2に格納されたデータをICカード3に書き込む場合には「CW: SI: 2= "Wc"」と記述する。

【0039】CFコマンドは、サービスを跨がった演算内容を記述するデータブロックを宣言する。例えば、サービスを跨がった演算内容をSFデータブロック1に記述する場合には、CF: CES\_FUNC=SF: 1」とする。そして、SFデータブロック1内に、例えば、「“Wc”=If (“Wc”>10) then (“Wc”-10; “Wd”=“Wc”\*0.08+“Wd”)」と記述する。本式は、サービスWcの残数が10よりも大きいときにWcの値を10減算し、Wcの8

%に相当するポイント数として蓄積ポイントとしてWdに加算する操作を表現している。

【0040】〔SAMチップ8〕図9は、図1に示すSAMチップ8の機能ブロック図である。図9に示すように、SAMチップ8は、ASPS通信インタフェース部60、外部メモリ通信インタフェース部61、バススクランブル部62、乱数発生部63、暗号・復号部64、記憶部65およびCPU66を有する。SAMチップ8は、耐タンパ性のモジュールである。

【0041】ASPS通信インタフェース部60は、図1に示すASPサーバ装置6との間のデータ入出力に用いられるインタフェースである。外部メモリ通信インタフェース部61は、外部メモリ7との間のデータ入出力に用いられるインタフェースである。バススクランブル部62は、外部メモリ通信インタフェース部61を介してデータを入出力する際に、出力するデータをスクランブルし、入力したデータをデスクランブルする。乱数発生部63は、認証処理を行う際に用いられる乱数を発生する。暗号・復号部64は、データの暗号化、並びに暗号化されたデータの復号を行う。記憶部65は、後述するように、CPU66によって用いられるタスク、プログラム、並びにデータを記憶する。CPU66は、後述するスクリプトダウンロードタスク、スクリプト解釈タスク、エンティティ生成タスク（ジョブ管理用データ作成タスク）およびICカード手続管理タスク（ジョブ管理用データ管理タスク）などのタスクを実行する。

【0042】以下、記憶部65に記憶されるタスク、プログラムおよびデータについて説明する。図10は、記憶部65に記憶されるタスク、プログラムおよびデータを説明するための図である。図10に示すように、スクリプトダウンロードタスク69、スクリプト解釈タスク70、エンティティ生成タスク71、ICカード手続管理用タスク72、ICカード操作用マクロコマンドスクリプトプログラム21\_\_1～21\_\_3、サービス定義テーブル20\_\_1～20\_\_3、ICカードエンティティテンプレートデータ30\_\_1～30\_\_3、ICカードエンティティデータ73\_\_x、入力用データブロック31\_\_x1、出力用データブロック32\_\_x2、ログ用データブロック33\_\_x3、並びに演算定義用データブロック34\_\_x4を記憶している。

【0043】スクリプトダウンロードタスク69は、図7に示すように、サービス定義テーブルデータ20\_\_1～20\_\_3を、例えば、各事業者のコンピュータからダウンロードし、これをSAMチップ8に取り込む。

【0044】スクリプト解釈タスク70は、各事業者毎に、サービス定義テーブルデータおよびスクリプトプログラムを用いて、ICカードエンティティプレートデータ、入力用データブロック、出力用データブロック、ログ用データブロックおよび演算定義用データブロックを生成する。各事業者毎に生成されるデータブロックの数

は特に限定されない。

【0045】エンティティ生成タスク71は、例えば、ASPサーバ装置6からエンティティ作成要求を受けると、ICカード3との間でポーリングを行った後に、当該ICカード3と事業者との間の手続き処理に用いるICカードエンティティデータを、当該事業者に対応するICカードエンティティプレートデータを用いて生成する。このとき、ICカードエンティティプレートデータがクラスとなり、当該クラスのインスタンスとして、ICカードエンティティデータが生成される。エンティティ生成タスク71によるICカードエンティティデータの生成処理について後に詳細に説明する。

【0046】ICカード手続管理用タスク72は、記憶部65内に存在する単数または複数のICカードエンティティデータ73\_xを用いて、ICカード3と事業者15\_1~15\_3との間の手続き処理を実行する。本実施形態では、複数のICカード3と事業者15\_1~15\_3との間で行われる複数の手続き処理が同時に進行する。ICカード手続管理用タスク72は、これら複数の手続き処理を並行して実行する。ICカード手続管理用タスク72は、一連の手続きを終了したICカードエンティティデータ73\_xを消去する。ICカード手続管理用タスク72の処理については後に詳細に説明する。

【0047】スクリプトプログラム21\_1~21\_2は、スクリプトダウンロードタスク69によって、例えば、外部メモリ7から入力され、記憶部65に記憶される。サービス定義テーブルデータ20\_1~20\_3は、スクリプトダウンロードタスク69によって、例えば、外部メモリ7から入力され、記憶部65に記憶される。

【0048】ICカードエンティティテンプレートデータ30\_1~30\_3は、スクリプト解釈タスク70によって生成され、それぞれの事業者に関する手続きのICカードエンティティデータ73\_xを生成する際のテンプレート（クラス）として用いられる。ICカードエンティティデータ73\_xは、エンティティ生成タスク71によって、ICカードエンティティテンプレートデータ30\_1~30\_3を例えばクラスとして用い、当該クラスのインスタンスとして生成される。

【0049】入力用データブロック31\_x1、出力用データブロック32\_x2、ログ用データブロック33\_x3および演算定義用データブロック34\_x4は、スクリプト解釈タスク70によって生成される。

【0050】以下、ICカードエンティティデータ73\_xについて説明する。ICカードエンティティデータ73\_xは、例えば、ASPサーバ装置6からICカード3と所定の事業者のアプリケーションプログラムを用いた処理の処理要求をSAMチップ8が受けたときに、SAMチップ8内のエンティティ生成タスク71が、既

に生成されている対応する事業者のICカードエンティティテンプレートデータを用いて生成する。

【0051】図11は、ICカードエンティティデータ73\_xのフォーマットを説明するための図である。図11に示すように、ICカードエンティティデータ73\_xは、管理用ポインタ情報80、エンティティID情報81、エンティティステータス情報（ステータスデータ）82、ICカード種別情報83、サービスタイプエレメント指定情報84、処理順番情報（処理順番データ）85、処理前情報86および処理後情報87を有する。

【0052】管理用ポインタ情報80には、記憶部65内でICカードエンティティデータ73\_xを管理するための双方向ポインタである。エンティティID情報81は、ICカードエンティティデータ73\_xの生成要求、進行状況の確認、削除などのICカードエンティティデータ73\_xを用いた一連の処理に用いられる。エンティティID情報81は、エンドユーザに渡される返り値ともなる。エンティティID情報81は一般的なファイルシステム上のファイルオープン時のディスクリプタに相当する。

【0053】エンティティステータス情報82は、ICカード3に関する手続きの進行状態を示す。ICカードエンティティデータ73\_xが持つ基本的な状態には、図12に示すように、ICカード3が利用できるサービスを調べる処理の状態（RS）、SAMチップ8がICカード3を認証する処理の状態（A1）、ICカード3がSAMチップ8を認証する処理の状態（A2）、ICカード3からデータ読み出す処理の状態（R）、ICカード3にデータ書き込む処理の状態（W）がある。本実施形態では、事業者を調べる処理、SAMチップ8がICカード3を認証する処理、ICカード3がSAMチップ8を認証する処理、ICカード3からデータ読み出す処理、並びにICカード3にデータ書き込む処理のそれぞれがジョブに対応している。当該ジョブは、後述するように、ICカード手続管理用タスク72によって、実行順番が決定される処理の単位になる。なお、A1、A2によって、ICカード3とSAMチップ8との間の相互認証処理が構成される。

【0054】また、本実施形態では、インターネット10での通信時間を考慮して、前述した各基本的な状態を図12の状態遷移図に示されるように、起動後（コマンド発行後）の状態と完了（応答受け取り後）状態とに分けて管理する。具体的には、インスタンス生成（ICカードエンティティデータ生成）状態、RS起動後状態、RS完了状態、A1起動後状態、A1完了状態、A2起動後状態、A2完了状態、R起動状態、R完了状態、W起動状態、W完了状態、並びにインスタンス（ICカードエンティティデータ）消去状態によって、ICカードエンティティデータ73\_xを用いた処理状態が管理され

る。

【0055】ICカード種別情報83は、当該ICカード3を発行した事業者を特定する情報である。ICカード種別情報83には、ICカードエンティティデータ73\_xの生成時に、前述したスクリプトプログラム内のC Iコマンドによって規定された情報が設定される。

【0056】サービスタイプエレメント情報84は、ICカードエンティティデータ73\_xを用いた処理で利用する、サービス定義テーブルデータ内で定義されたサービスのサービスタイプエレメントを示す。サービスタイプエレメント情報84には、ICカードエンティティデータ73\_xの生成時に、前述したスクリプトプログラム内のC Sコマンドで指定された単数または複数のサービスタイプエレメントが設定される。

【0057】処理順番情報85は、ICカードエンティティデータ73\_xを用いた処理で利用するサービス（ジョブ）を実行する順番、すなわち、図12に示す遷移状態を示す。すなわち、処理順番情報85は、サービスタイプエレメントを用いて、ICカード3の基本的な操作に対応するジョブの実行順番を示す。ここで、ジョブは、前述したように、図12に示すRS、A1、A2、R、Wに相当する。ICカード3への具体的操作は、ジョブを用いて指定された処理順番により実現される。例えば、相互認証無しの読み込みのみのICカード3を用いた処理については、処理順番情報85には「RS→R」が設定される。また、相互認証有りの読み込みおよび書き込みの場合には、処理順番情報85には、「RS→A1→A2→R→W」が設定される。処理順番情報85には、ICカードエンティティデータ73\_xの生成時に、前述したスクリプトプログラム内のC Sコマンド内で指定されたサービスエレメントの順番に対応する図12に示すジョブの順番が設定される。

【0058】処理前情報86には、ASPサーバ装置6側から、ICカードエンティティデータ73\_xを用いた処理を行うための管理用データが設定される。。例えば、処理前情報86には、SFデータブロック内に指定されたサービスの演算式のポイントが設定される。また、サービス間演算機能が定義されていない場合には、処理前情報86には、要求処理金額が設定される。例えば、決済の場合であれば、課金額や付与ポイント数などに関する状態が設定される。

【0059】処理後情報87は、ASPサーバ装置6側で必要な、ICカードエンティティデータ73\_xの処理結果のデータが設定される。例えば決済の場合であれば、決済の正常終了の有無などを示すデータが設定される。

【0060】以下、図10に示すICカード手続管理用タスク72による、複数のICカードエンティティデータ73\_xを用いて、複数のICカード3に係わる処理を行う手順を説明する。ICカード手続管理用タスク7

2は、例えば、図9に示すSAMチップ8のCPU66上で常に起動されている。図13は、ICカード手続管理用タスク72が行う処理のフローチャートである。

ステップST1：ICカード手続管理用タスク72は、記憶部65内に存在する複数のICカードエンティティデータ73\_xのうち、次に処理を実行する一つのICカードエンティティデータ73\_xを選択する。当該ICカードエンティティデータ73\_xの選択方法は、記憶部65内に存在するICカードエンティティデータ73\_xを順番に選択してもよいし、優先順位を付けて高い優先順位のものを優先的に選択してもよい。

【0061】、ステップST2：ICカード手続管理用タスク72は、ステップST1で選択したICカードエンティティデータ73\_xのジョブが既に起動されているか否かを判断し、起動されていると判断した場合にはステップST5の処理に進み、起動されていないと判断した場合にはステップST3の処理に進む。

【0062】ステップST3：ICカード手続管理用タスク72は、ステップST1で選択したICカードエンティティデータ73\_xの図11に示すエンティティステータス情報82から、当該エンティティデータに関する処理が図12に示す状態遷移図の何れの状態にあるかを判断し、処理順番情報85から、次に実行するジョブを決定する。このとき処理順番情報85には、前述したように、サービス定義テーブルデータに設定されたサービスエレメントを用いてジョブの実行順番が規定されている。

【0063】ステップST4：ICカード手続管理用タスク72は、ステップST3で選択したジョブを起動する。ICカード手続管理用タスク72は、図7を用いて前述した入力用データブロック31\_x1、出力用データブロック32\_x2、ログ用データブロック33\_x3および演算定義用データブロック34\_x4のうち、当該ジョブに関係するデータブロックを用いて当該ジョブを実行する。

【0064】このとき、ICカード手続管理用タスク72は、ジョブの実行に当たってICカード3にコマンドを発行する場合に、当該ジョブに対応するサービスエレメントをキーとしてサービス定義テーブルデータを検索し、当該サービスエレメントに対応するサービス番号（ICカード3が解釈可能なICカード3の操作コマンド）を得る。そして、ICカード手続管理用タスク72は、当該得られたサービス番号を用いてICカード3にコマンドを発行する。また、ICカード手続管理用タスク72は、図4を用いて説明したように、ICカード3のIC3aの記憶領域へのアクセスに鍵情報が必要な場合には、当該ジョブに対応するサービスエレメントをキーとしてサービス定義テーブルデータを検索し、当該サービスエレメントに対応する鍵情報を得る。そして、ICカード手続管理用タスク72は、当該鍵情報を用い

て、ICカード3との間で相互認証、データの暗号化および復号などの処理を行い、ICカード3の所定の記憶領域にアクセスを行う権限を得る。

【0065】ステップST5：ステップST5が行われるのは、ICカード手続管理用タスク72が、ICカード3にコマンドを発行し、ICカード3の処理結果を待っているときである。ICカード手続管理用タスク72は、ICカード3から処理結果を受け取ると、これをICカードエンティティデータ73\_xに設定する。

【0066】ステップST6：ICカード手続管理用タスク72は、図11に示すICカードエンティティデータ73\_xのエンティティステータス情報82を更新する。

【0067】このように、本実施形態では、ICカード手続管理用タスク72によって、SAMチップ8内に存在する複数のICカード3についてのICカードエンティティデータ73\_xを順に選択しながら、複数のICカード3についての処理を並行して行う。そのため、SAMチップ8は、複数のICカード3を用いた手続きの処理要求を受けた場合でも、これらの処理を同時に進行することができる。

【0068】以下、図1に示す通信システム1の全体動作について説明する。図14および図15は、図1に示す通信システム1の全体動作を説明するための図である。

【0069】ステップST21：事業者15\_1～15\_3あるいはこれら事業者の依頼を受けた者が、当該事業者がICカード3を用いて行う取引についての処理を記述したスクリプトプログラム21\_1、21\_2、21\_3を、例えば、図1に示すパーソナルコンピュータ16\_1、16\_2、16\_3上で作成する。また、SAMチップ8の管理者が、事業者15\_1～15\_3のそれぞれに対応するサービス定義テーブルデータ20\_1、20\_2、20\_3を作成する。

【0070】ステップST22：ステップST21で作成されたサービス定義テーブルデータ20\_1、20\_2、20\_3が外部メモリ7に記憶される。また、ステップST21で作成されたスクリプトプログラム21\_1、21\_2、21\_3が、パーソナルコンピュータ16\_1、16\_2、16\_3から、インターネット10、ASPサーバ装置6およびSAMチップ8を介して、外部メモリ7にダウンロードされる。当該ダウンロードの処理は、図7に示すように、SAMチップ8内のスクリプトダウンロードタスク69によって管理される。

【0071】ステップST23：図7に示すSAMチップ8内のスクリプト解釈タスク70によって、各事業者毎に、サービス定義テーブルデータおよびスクリプトプログラムを用いて、ICカードエンティティプレートデータ、入力用データブロック、出力用データブロック、

ログ用データブロックおよび演算定義用データブロックが生成される。これら生成されたデータは、図9に示すSAMチップ8の記憶部65に格納される。

【0072】ステップST24：ユーザにICカード3が発行される。図4に示すように、ICカード3のIC3aには、ユーザが契約を行った事業者との取り引きに用いられる鍵情報が記憶されている。なお、ユーザと事業者との間の契約は、ICカード3の発行後に、インターネット10などを介して行ってもよい。

【0073】ステップST25：例えば、ユーザがパーソナルコンピュータ5を用いてインターネット10を介してサーバ装置2にアクセスを行い、商品を購入しようとした場合に、サーバ装置2がインターネット10を介してASPサーバ装置6に処理要求を出す。ASPサーバ装置6は、サーバ装置2から処理要求を受けると、インターネット10を介してパーソナルコンピュータ5にアクセスを行う。そして、図16(A)に示すように、カードリーダー・ライタ4が出したICカード3についての処理要求が、パーソナルコンピュータ5、インターネット10およびASPサーバ装置6を介してSAMチップ8に送信される。

【0074】ステップST26：ASPサーバ装置6からSAMチップ8にエンティティ作成要求が出される。当該エンティティ作成要求には、ICカード3の発行元を示す情報が格納されている。

【0075】ステップST27：SAMチップ8は、エンティティ作成要求を受けると、図16(B)に示すように、ICカード3との間でボーリングを行う。

【0076】ステップST28：SAMチップ8のエンティティ生成タスク71は、ボーリング終了後に、SAMチップ8内に存在するICカードエンティティデータ73\_xの数が、スクリプトプログラムのSCコマンドによって規定された最大数以内であるか否かを判断し、最大数以内であればステップST29の処理に進み、そうでない場合には処理を終了する。

【0077】ステップST29：エンティティ生成タスク71が、例えば、エンティティ作成要求に格納されたICカード3の発行元を示す情報に基づいて、何れの事業者のICカードエンティティプレートデータを用いるかを特定し、当該特定したICカードエンティティプレートデータを用いて、ICカードエンティティデータ73\_xを生成する。これは、図12に示すインスタンス生成に対応している。

【0078】ステップST30：SAMチップ8からASPサーバ装置6に、ステップST29で生成したICカードエンティティデータ73\_xのエンティティIDが出力される。

【0079】ステップST31：SAMチップ8のICカード手続管理用タスク72によって、ICカード3で利用可能なサービスが調べられる。これは、図12に示

すジョブRSに対応した処理である。

【0080】ステップST32：SAMチップ8のICカード手続管理用タスク72がICカード3の正当性を認証する。これは、図12に示すジョブA1に対応した処理である。

【0081】ステップST33：ICカード3がSAMチップ8の正当性を認証する。これは、図12に示すジョブA2に対応した処理である。ステップST32、ST33によって、ICカード3とSAMチップ8との間の相互認証が行われる。これは、図16(C)に対応している。

【0082】ステップST34：SAMチップ8のICカード手続管理用タスク72が、ICカード3との間で、手続きに必要なデータの読み書きを行う。これは、図12に示すジョブR、W、並びに図16(D)、

(E)に対応した処理である。また、ICカード手続管理用タスク72は、ICカードエンティティデータ73\_xの処理前情報86に基づいて特定した演算式を用いて、ICカード3から読み出したデータを用いて所定の演算処理を行う。

【0083】ステップST35：図16(F)に示すように、SAMチップ8のICカード手続管理用タスク72が、ステップST34の処理結果をASPサーバ装置6に出力する。

【0084】ステップST36：例えば、ICカード手続管理用タスク72が、ICカードエンティティデータ73\_xを消去する。

【0085】以上説明したように、通信システム1によれば、ICカード3との間で発生する手続き処理毎にICカードエンティティデータ73\_xを生成し、ICカード手続管理用タスク72によって、複数のICカードエンティティデータ73\_xを用いて、複数のICカード3についての処理を同時に進行することができる。また、認証システム1によれば、ICカード3についての処理に実際に用いられているICカードエンティティデータ73\_xを記憶部65に記憶すれば良いため、記憶部65の記憶領域を効率的に利用できる。また、認証システム1によれば、図12に示すように、ICカード手続管理用タスク72が処理するジョブの実行状態を、起動後状態と完了状態とに分離して管理するため、一のジョブの実行を開始後にICカード3からのデータを待っている状態で、他のジョブに関する処理を開始できる。そのため、インターネット10を介してICカード3との間でデータを送受信することによる待ち時間を無くすることができる。

【0086】また、認証システム1によれば、サービス定義テーブルデータ内に、各事業者が提供するサービスの種類を示す名前であるサービスタイプエレメント、ICカード3内で用いられる当該サービスの番号、並びに当該サービスを提供する際に用いられる鍵情報をサー

ビス定義テーブルデータ内に記述し、これを外部メモリ7に保持する。そのため、SAMチップ8の開発者でない、事業者15\_1～15\_3が、SAMチップ8上で動作する自らのアプリケーションプログラムを、スクリプトプログラム21\_1、21\_2、21\_3を作成してSAMチップ8を介して外部メモリ7にダウンロードすることでカスタマイズできる。すなわち、鍵情報やICカード3を直接操作する操作コマンドなどの秘匿性の高い情報を事業者15\_1～15\_3に知らせることなく、これらの事業者が自らのアプリケーションプログラムをカスタマイズできる。また、事業者は、アプリケーションプログラムをカスタマイズする際に、鍵情報やカード操作コマンドを知る必要がないため、事業者の負担が軽減される。また、認証システム1によれば、複数のサービスにまたがった処理内容を定義できるため、ICカード3側で許容されると同時に実行されるサービスの範囲内で、複数のサービスを組み合わせた多様なサービスを提供できる。また、認証システム1によれば、データブロックの概念を導入することで、ICカード3との間で入出力されるデータ、並びにログデータの管理が容易に行える。

【0087】図17は、図9に示すSAMチップ8の機能ブロックをより具体的に示した機能ブロック図である。図9に示すように、SAMチップ8は、内部バス90を介して、ASPS通信インタフェース部60、外部メモリ通信インタフェース部61、バススクランブル部62、乱数発生部63、暗号・復号部64、記憶部65およびCPU66が接続されている。

【0088】図17に示すSAMチップ8では、例えば図18に示すように、内部バス90に接続されたカードI/F部91を、SAMチップ8の外部のRF送受信部92に接続し、RF送受信部92のアンテナ92aを介して、ICカード3との間で非接触方式でデータを送受信してもよい。

【0089】

【発明の効果】以上説明したように、本発明によれば、秘匿性の高い情報をユーザに知らせることなく、サーバ装置で実行するユーザのアプリケーションプログラムを当該ユーザが作成およびカスタマイズできるデータ処理方法および半導体回路を提供できる。

【図面の簡単な説明】

【図1】図1は、本発明の実施形態の通信システムの全体構成図である。

【図2】図2は、図1に示すSAMチップのソフトウェア構成を説明するための図である。

【図3】図3は、図1に示すICカードのICの機能ブロック図である。

【図4】図4は、図3に示す記憶部に記憶される情報を説明するための図である。

【図5】図5は、図1に示すSAMユニットの外部メモ

りに記憶されている情報を説明するための図である。

【図6】図6は、図5に示すサービス定義テーブルデータを説明するための図である。

【図7】図7は、図5に示すサービス定義テーブルデータおよびスクリプトプログラムを用いたSAMチップ内の処理を説明するための図である。

【図8】図8は、スクリプトプログラムで用いられるコマンドを説明するための図である。

【図9】図9は、図1に示すSAMチップの機能ブロック図である。

【図10】図10は、図9に示す記憶部に記憶されるデータを説明するための図である。

【図11】図11は、SAMチップで生成されるICカードエンティティデータのフォーマットを説明するための図である。

【図12】図12は、図11に示すICカードエンティティデータの状態遷移図である。

【図13】図13は、図10に示すICカード手続管理タスクの処理手順を説明するための図である。

【図14】図14は、図1に示す通信システムの全体動作を説明するための図である。

【図15】図15は、図1に示す通信システムの全体動作を説明するための図である。

【図16】図16は、ICカードとSAMチップとの間の通信プロトコルを説明するための図である。

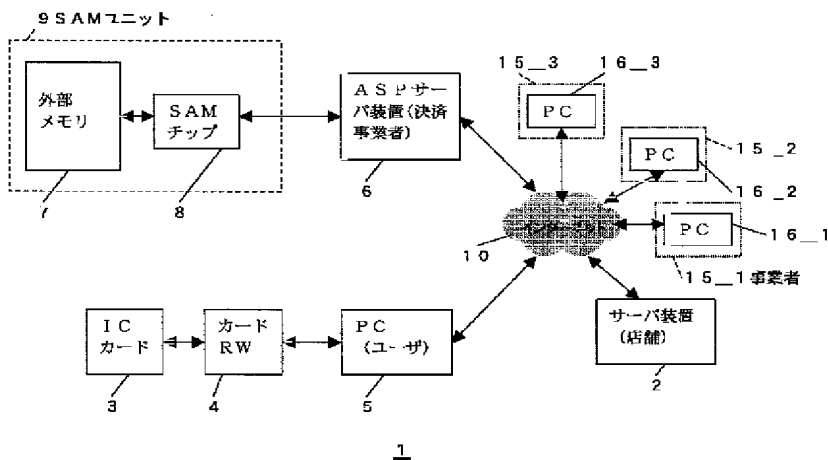
【図17】図17は、図9に示すSAMチップの機能ブロックをより具体的にした機能ブロック図である。

【図18】図18は、SAMチップのその他の使用形態を説明するための図である。

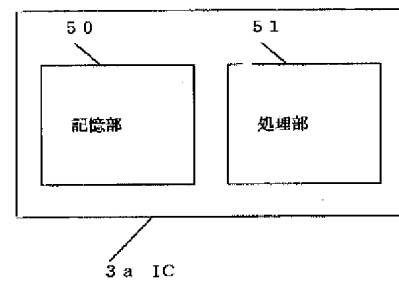
【符号の説明】

1…通信システム、2…サーバ装置、3…ＩＣカード、  
4…カードリーダー・ライター、5…パーソナルコンピュータ、6…ＡＳＰサーバ装置、7…外部メモリ、8…ＳＡ  
Ｍチップ、9…ＳＡＭユニット、10…インターネット、15\_1、15\_2、15\_3…クレジットカード  
事業者、16\_1、16\_2、16\_3…パーソナルコ  
ンピュータ

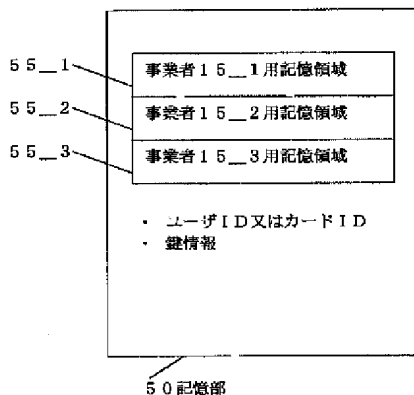
【例 1】



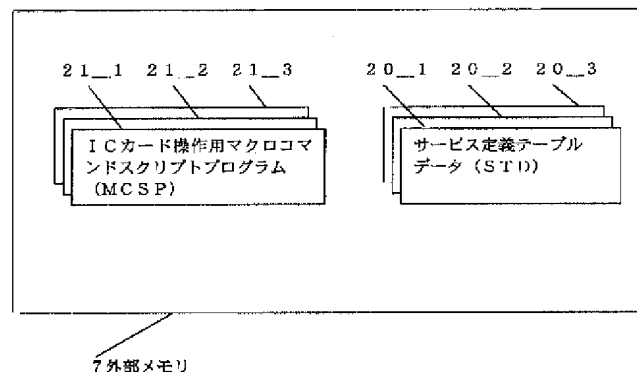
【例 3】



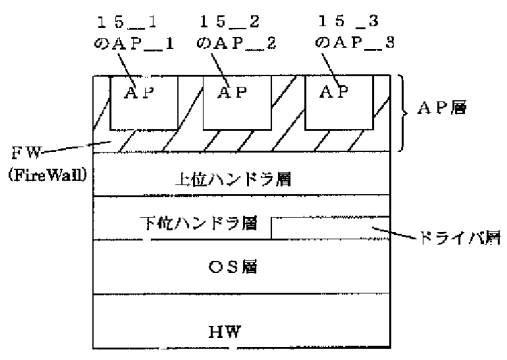
【図4】



【図5】



【図2】



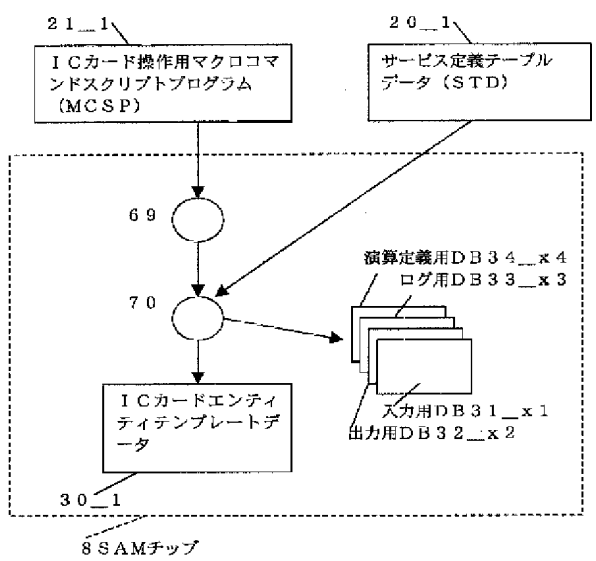
SAMチップのソフトウェア構成

【図6】

サービスタイプ エレメント	アドレス	サービス 番号	鍵 バージョン	鍵情報
Rc	...	...	...	...
Rd	...	...	...	...
Wc	...	...	...	...
Wd	...	...	...	...

SDT20\_1

【図7】



【図11】

80	管理用ポインタ情報
81	エンティティID情報
82	エンティティステータス情報
83	ICカード種別情報
84	サービスタイプエレメント指定情報
85	処理順番情報
86	処理前情報 (要求金額付与ポイント数)
87	処理後情報 (最終成否)

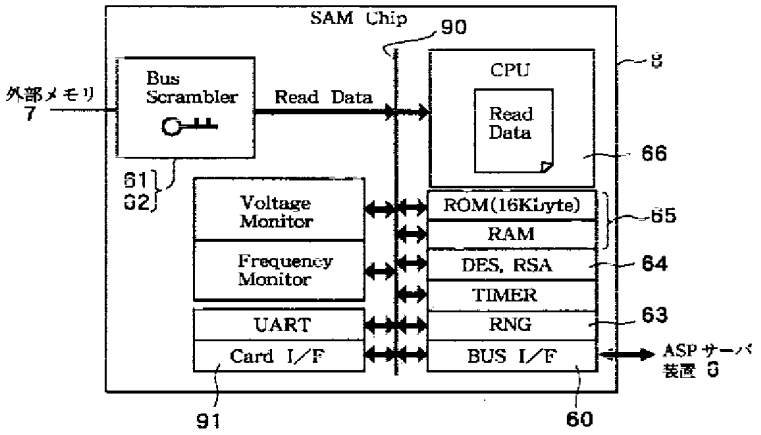
ICカードエンティティデータ

【図8】

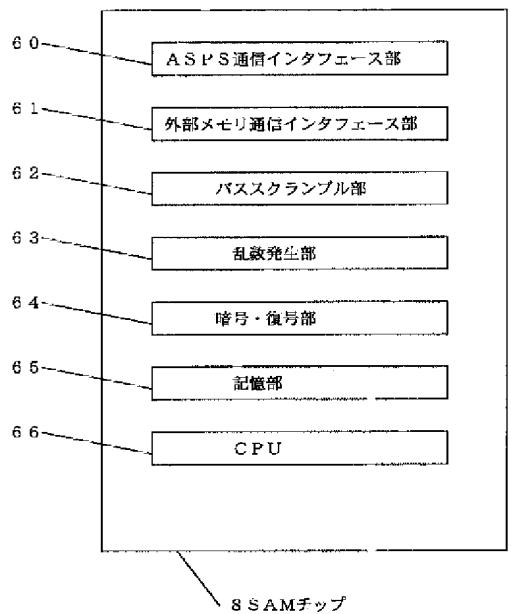
- SCコマンド: 最大同時処理枚数宣言
- SOコマンド: カードから読み取るデータ格納先の宣言
- SIコマンド: カードへ書き込むデータ格納先の宣言
- SLコマンド: カード操作時のログデータ格納先の宣言
- CIコマンド: カード読行体宣言
- CSコマンド: カードサービスタイプエレメント宣言。SDTで定義された名前を引用
- CRコマンド: 読み込みの操作。カードサービスタイプを基にカード上の実データ格納先の指示を行う
- CWコマンド: 書き込みの操作。カードサービスタイプを基にカード上の実データ格納先の指示を行う
- CSコマンド: サービスタイプエレメント相互間の関連づけ機能
- CFコマンド: 関連付け関数の実定義機能

MCSPに用いられるコマンド

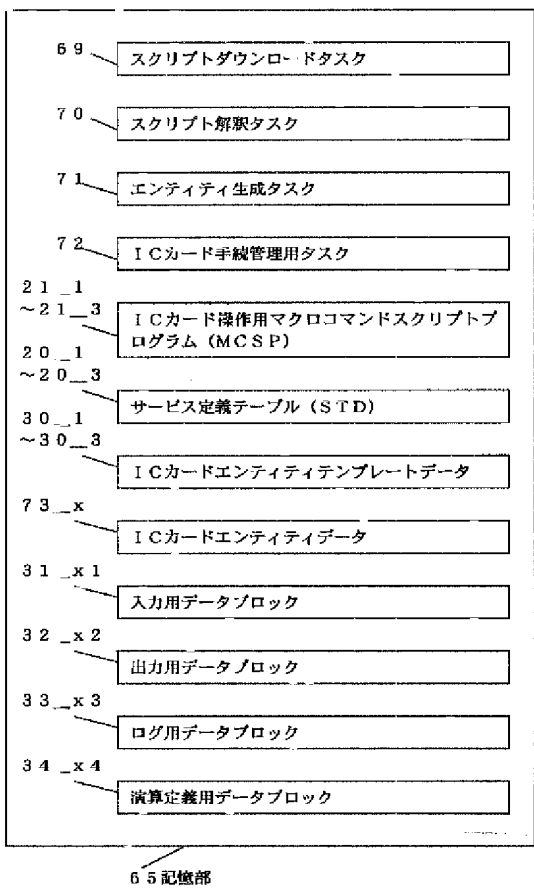
【図17】



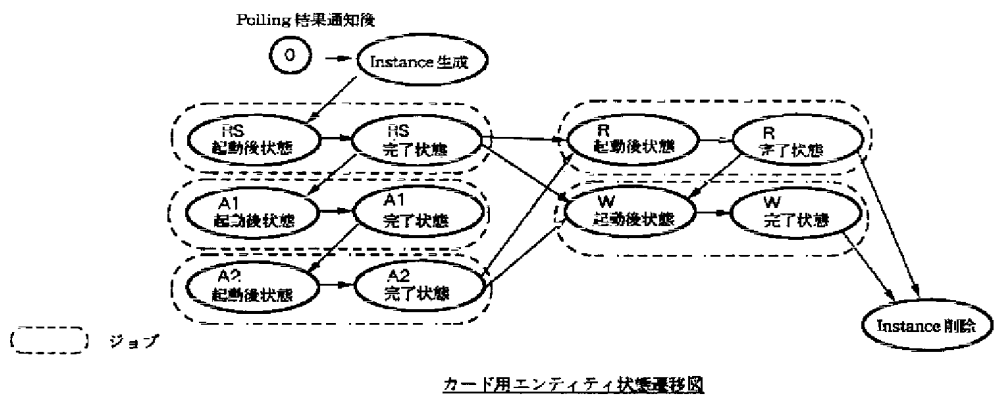
【図 9】



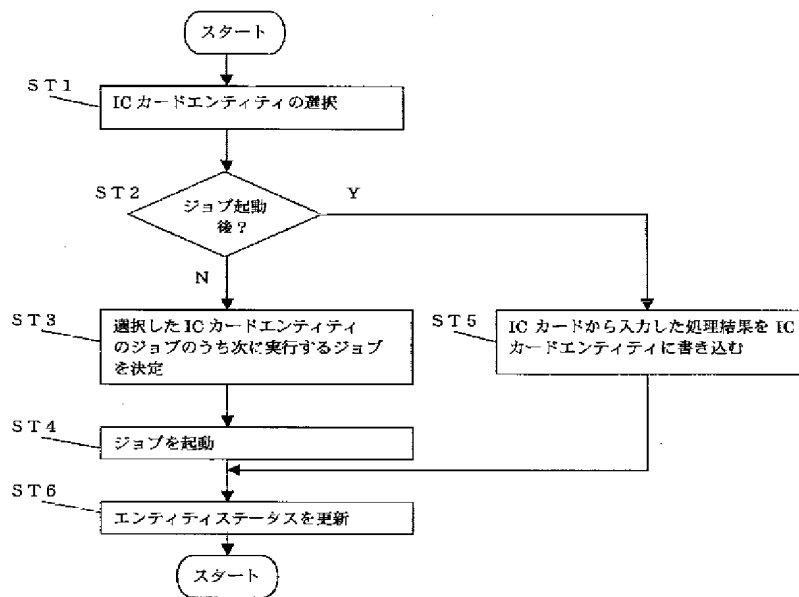
【図 10】



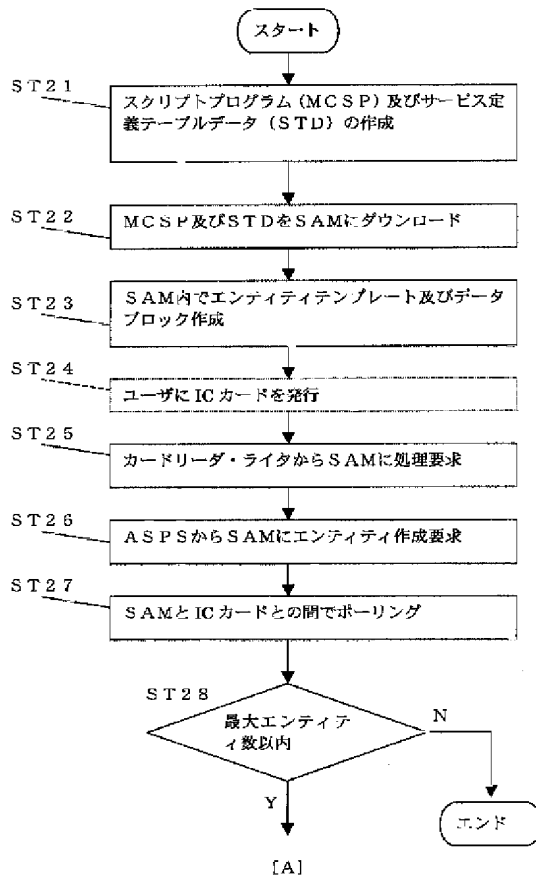
【図 12】



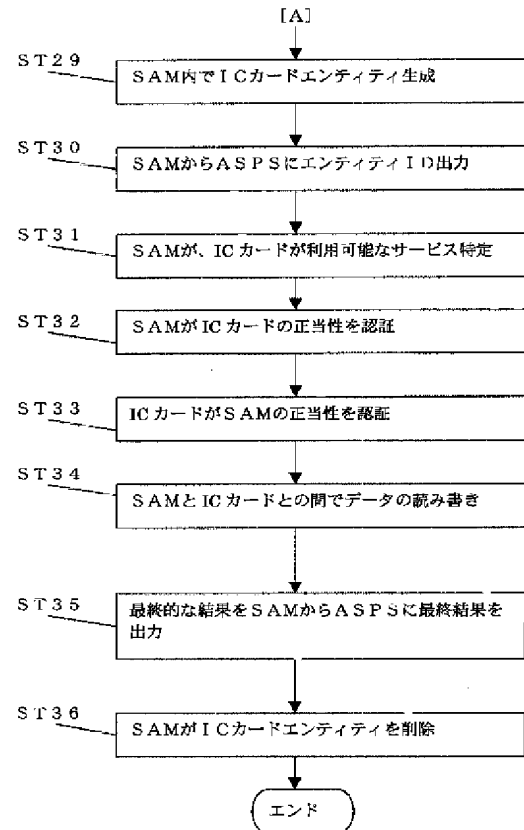
【図13】



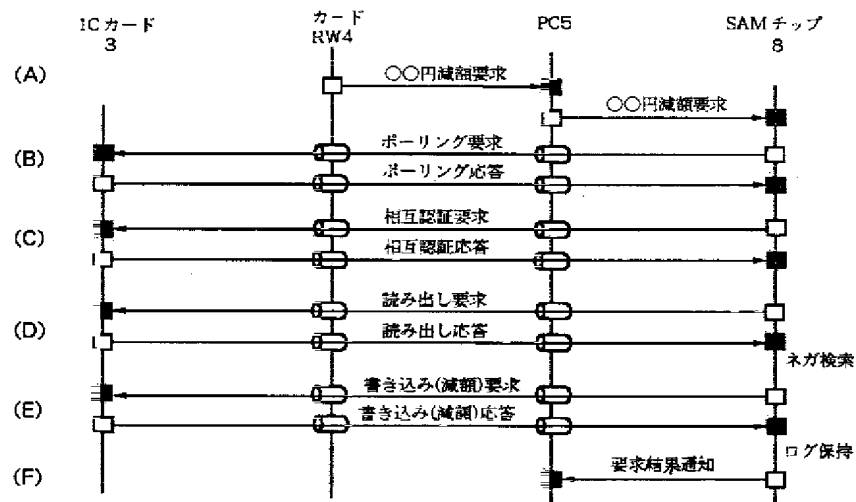
【図14】



【図15】



【 図 1 6 】



【 図 1 8 】

